(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 757 978**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 16243**

(51) Int Cl⁶ : **G 06 K 19/073**, G 11 C 16/02

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 27.12.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 03.07.98 Bulletin 98/27.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SCHLUMBERGER INDUSTRIES SA SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** FRANCHI OLIVIER.

(73) **Titulaire(s) :** .

(74) **Mandataire :** SCHLUMBERGER INDUSTRIES.

## (54) PROCEDE DE SECURISATION D'UNE DONNEE DANS UNE MEMOIRE REINSCRIPTIBLE.

(57) Procédé de sécurisation d'une donnée dans une mémoire réinscriptible d'un composant électronique apte à effectuer des opérations susceptibles de modifier ladite donnée.

Selon l'invention, ledit procédé comporte les étapes suivantes:

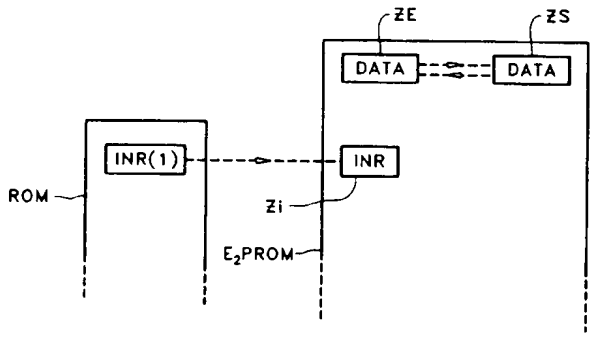
a) dans une phase d'initialisation:

- définir dans ladite mémoire réinscriptible (E2PROM):
  . une zone (ZE) d'écriture de la donnée,
  . une zone (ZS) de sauvegarde de la donnée,
  . une zone (Zi) dans laquelle est inscrite une valeur d'un indicateur (INR(Zi)) de restauration,
- définir dans une mémoire morte (ROM) une valeur (INR(1)), dite restauration, de l'indicateur (INR(Zi)), indiquant qu'une restauration de la donnée doit être effectuée,
- définir une valeur (INR(0)), dite d'effacement, de l'indicateur (INR(Zi)) de restauration,

b) à chaque accès de ladite zone (ZE) d'écriture:

- lire dans la zone (Zi) la valeur dudit indicateur (INR(Zi)),
- si la valeur de l'indicateur de restauration est égale à ladite valeur de restauration, effectuer une restauration de la donnée et inscrire dans la zone (Zi) ladite valeur (INR(0)) d'effacement.

Application aux cartes à mémoire électronique.




FR 2 757 978 - A1

# PROCÉDÉ DE SÉCURISATION D'UNE DONNÉE DANS UNE MÉMOIRE RÉINSCRIPTIBLE

La présente invention concerne un procédé de sécurisation d'au moins une donnée dans une mémoire réinscriptible d'un composant électronique, ledit composant électronique étant apte à effectuer des opérations susceptibles de modifier ladite donnée.

L'invention trouve une application particulièrement avantageuse dans le domaine des cartes à mémoire électronique, notamment les cartes connues sous le nom de porte-monnaie électroniques.

D'une manière générale, les cartes à mémoire électronique précitées utilisent des mémoires du type EEPROM ou flash EPROM qui ont le double avantage d'être non volatiles et électriquement effaçables, donc réinscriptibles. Toutefois, dans certaines applications, il arrive que ces mémoires soient corrompues en raison, notamment, d'une interruption accidentelle de l'alimentation électrique en cours d'opération, entraînant la perte des données antérieures sans inscription de nouvelles données.

Ce dernier risque est particulièrement important dans les applications, telles que les cartes à mémoire électronique, où ladite mémoire est embarquée dans un objet dépendant d'une source d'alimentation extérieure dont il peut être séparé à tout moment par arrachement volontaire ou non.

Des solutions à ce problème ont déjà été décrites. Elles consistent généralement, lorsqu'on veut modifier les valeurs d'une donnée, à inscrire les valeurs courantes successives de ladite donnée dans des zones différentes de la mémoire. En conséquence, il est nécessaire de programmer le pointeur servant d'indicateur de manière à ce qu'il puisse désigner la zone dans laquelle est inscrite la dernière valeur courante de la donnée.

L'inconvénient de ce type de procédé est qu'il nécessite plusieurs opérations d'inscription qui peuvent être chacune le siège d'une corruption. Le logiciel gérant les inscriptions dans la

mémoire doit donc être complexe et, de là, consommateur de temps et d'espace mémoire.

Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de sécurisation d'au moins une donnée dans une mémoire réinscriptible d'un composant électronique, ledit composant électronique étant apte à effectuer des opérations susceptibles de modifier ladite donnée, procédé qui permettrait à coup sûr d'éviter les inconvénients liés à toute interruption d'alimentation du composant quel que soit le moment où se produit cette interruption dans le déroulement de l'opération.

La solution au problème technique posé consiste, selon la présente invention en ce que ledit procédé comporte les étapes consistant à :

a) dans une phase d'initialisation :

- définir dans ladite mémoire réinscriptible :
  - une zone d'écriture de la donnée,
  - une zone de sauvegarde de la donnée, dans laquelle est inscrite une valeur non corrompue de ladite donnée,
  - une zone d'indication de restauration, dans laquelle est inscrite une valeur d'un indicateur de restauration,
- définir dans une mémoire morte du composant électronique une valeur, dite de restauration, de l'indicateur de restauration, indiquant qu'une restauration de la donnée doit être effectuée suite à une corruption d'écriture de ladite donnée,
- définir une valeur, dite d'effacement, de l'indicateur de restauration, différente de la valeur de restauration,

b) à chaque accès de ladite zone d'écriture :

- lire dans la zone d'indication de restauration la valeur dudit indicateur de restauration,
- si la valeur de l'indicateur de restauration est égale à ladite valeur de restauration, effectuer une restauration de la donnée en inscrivant dans la zone d'écriture la valeur de la donnée inscrite dans ladite zone de sauvegarde, et inscrire

dans la zone d'indication de restauration ladite valeur d'effacement de l'indicateur de restauration.

Ce type de procédé peut être mis en oeuvre lorsque l'on désire seulement accéder à la zone d'écriture, pour simple lecture de la valeur qui y est inscrite, comme le crédit disponible dans un porte-monnaie électronique.

Lorsque l'on veut maintenant modifier la valeur inscrite dans la zone d'écriture, suite à une transaction effectuée au moyen dudit porte-monnaie électronique par exemple, il est prévu que le procédé de sécurisation de l'invention comporte en outre les étapes consistant, à chaque mise à jour de ladite zone d'écriture, à :

- sauvegarder la valeur de ladite donnée inscrite dans la zone d'écriture en l'inscrivant dans la zone de sauvegarde,
- inscrire dans la zone d'indication de restauration ladite valeur de restauration,
- inscrire dans la zone d'écriture une nouvelle valeur de la donnée, résultant de l'opération,
- inscrire dans la zone d'indication de restauration ladite valeur d'effacement de l'indicateur de restauration.

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est une représentation schématique des zones-mémoire d'un composant électronique sécurisé au moyen du procédé de l'invention.

La figure 2 est un schéma synoptique d'un premier mode de mise en oeuvre du procédé de l'invention.

La figure 3 est un schéma synoptique d'un deuxième mode de mise en oeuvre du procédé de l'invention.

Sur la figure 1 sont représentées de manière schématique des zones-mémoire d'un composant électronique appartenant, par exemple, à un porte-monnaie électronique destiné à effectuer des transactions financières avec un terminal prévu à cet effet.

Comme l'indique la figure 1, ledit composant électronique comprend une mémoire réinscriptible EEPROM, qui d'ailleurs

pourrait être tout aussi bien une mémoire flash EPROM, dans laquelle doit être inscrite de manière sécurisée une donnée DATA susceptible d'être modifiée au cours de l'opération réalisée par le composant électronique. Dans le cas d'une transaction financière, cette donnée peut être le crédit disponible dans le porte-monnaie ainsi que le nombre de transactions effectuées, lequel s'incrémente d'une unité à chaque transaction validée.

Dans une phase d'initialisation, le procédé de sécurisation de la donnée DATA consiste à définir dans la mémoire réinscriptible EEPROM trois zones distinctes, respectivement référencées ZE, ZS et Zi.

La zone ZE est une zone d'écriture dans laquelle est inscrite toute nouvelle valeur de la donnée DATA. Le but du procédé de l'invention étant précisément d'éviter les inconvénients liés à une corruption d'écriture de ladite donnée dans la zone ZE d'écriture, due par exemple à une coupure de l'alimentation électrique du composant électronique, il est prévu une zone ZS de sauvegarde de la donnée, destinée à recevoir, selon un processus qui sera décrit plus loin, une valeur de la donnée dont il peut être établi avec certitude qu'elle est non corrompue. Enfin, dans la zone notée Zi, dite d'indication de restauration, est inscrite la valeur prise par un indicateur INR(Zi) de restauration au cours du déroulement du procédé de sécurisation de l'invention. Plus particulièrement, ledit indicateur INR(Zi) de restauration peut prendre une valeur INR(1), dite de restauration, indiquant qu'une restauration de la donnée doit être effectuée à partir de la zone ZS de sauvegarde, suite à une corruption d'écriture de la donnée. Cette valeur INR(1), par exemple 87 en numérotation hexadécimale, est inscrite définitivement dans une mémoire morte ROM du composant électronique. Est également définie une valeur INR(0) d'effacement, différente de INR(1), de l'indicateur INR(Zi) de restauration. La valeur INR(0) est prise par exemple égale à 00 et est affectée à l'indicateur INR(Zi) sur simple instruction de programmation.

Sur la figure 2 est représenté un schéma synoptique d'un premier mode de mise en oeuvre du procédé de sécurisation de

l'invention dans le cas d'un simple accès à la zone ZE d'écriture, pour lecture de la donnée DATA par exemple. Comme l'indique la partie centrale de la figure 2, le procédé de sécurisation consiste à lire dans la zone Zi d'indication de restauration la valeur dudit indicateur INR(Zi) de restauration. Puis, si la valeur de INR(Zi) est égale à ladite valeur INR(1) de restauration, ce qui indique que la valeur de la donnée dans la zone ZE d'écriture est corrompue, on effectue une restauration de la donnée en inscrivant dans ladite zone d'écriture la valeur de la donnée inscrite dans la zone ZS de sauvegarde, et on inscrit ensuite dans la zone Zi ladite valeur INR(0) d'effacement de l'indicateur de restauration, montrant ainsi que la valeur de la donnée inscrite dans la zone ZE d'écriture à laquelle on veut accéder est une valeur non corrompue et qu'il n'est pas nécessaire d'effectuer une restauration à partir de la zone ZS de sauvegarde. Le tableau de droite de la figure 2 illustre ce processus dans le cas où la valeur DATA(n-2) de la donnée lors d'une $(n-2)^{ième}$ transaction n'a pas été corrompue et normalement sauvegardée dans la zone ZS, mais où une corruption s'est produite au cours de la $(n-1)^{ième}$ transaction, portant l'indicateur INR(Zi) à la valeur INR(1) de restauration, la valeur de la donnée dans la zone ZE d'écriture étant incertaine.

On observera que, si lors de la restauration de la donnée DATA (n-2) de la zone ZS de sauvegarde vers la zone ZE d'écriture une coupure d'alimentation se produisait, cela n'aurait aucune conséquence néfaste puisque, l'indicateur INR(Zi) restant égal à sa valeur INR(1) de restauration, une nouvelle restauration aurait lieu à la demande suivante d'accès à la zone ZE d'écriture.

Par contre, on peut voir sur le tableau de gauche de la figure 2 que si, à l'inverse, la $(n-1)^{ième}$ transaction s'est effectuée normalement, sans corruption, la dernière valeur DATA (n-1) est inscrite dans la zone ZE d'écriture et que , l'indicateur INR(Zi) ayant la valeur INR(0), l'accès à la zone ZE se fera directement, sans restauration.

La figure 3 représente un schéma synoptique d'un deuxième mode de mise en oeuvre du procédé de sécurisation de l'invention

dans le cas d'une mise à jour de la zone ZE d'écriture, lorsque, par exemple, il faut modifier le crédit disponible d'un porte monnaie électronique à la suite d'une transaction financière.

Cette opération de mise à jour débute d'abord par un accès à la zone ZE d'écriture, conformément au processus qui vient d'être décrit, puis, comme le montre plus particulièrement la partie centrale de la figure 3, on procède à une sauvegarde de la donnée inscrite dans la zone ZE d'écriture en l'inscrivant dans la zone ZS de sauvegarde. Cette sauvegarde est sans effet sur le contenu des zones ZE et ZS si, initialement, l'indicateur INR(Zi) avait la valeur INR(1) (tableau de droite de la figure 3). Par contre, si la valeur initiale INR(Zi) est INR(0) (tableau de gauche de la figure 3), la sauvegarde de la zone ZE a pour effet de remplacer la valeur DATA (n-2) dans la zone ZS par la valeur DATA (n-1) contenue dans ZE. On remarque qu'une corruption survenant lors de la sauvegarde est sans conséquence puisque, d'une part, elle n'affecte que la zone ZS de sauvegarde et que, d'autre part, l'indicateur INR(Zi) étant différent de INR(1), aucune restauration ne sera réalisée au début de la transaction suivante.

Après la sauvegarde de la zone ZE d'écriture, on inscrit dans la zone Zi de restauration ladite valeur INR(1) de restauration. Puis, la $n^{ième}$ transaction est effectuée en inscrivant dans la zone ZE la nouvelle valeur DATA (n) de la donnée. Si une interruption d'alimentation électrique du composant a lieu au cours de cette inscription une restauration de la donnée sera automatiquement effectuée puisque la valeur de l'indicateur INR(Zi) étant la valeur INR(1) de restauration, la dernière valeur non corrompue de la donnée, DATA(n-1) ou DATA (n-2), sera inscrite dans la zone ZE au cours de la $(n-1)^{ième}$ transaction.

Enfin, si l'écriture de la nouvelle donnée DATA(n) dans la zone ZE s'est effectuée sans corruption, on inscrit dans la zone Zi ladite valeur INR(0) d'effacement de l'indicateur de restauration, aucune restauration n'étant nécessaire au début de la $(n+1)^{ième}$ transaction.

## REVENDICATIONS

1. Procédé de sécurisation d'au moins une donnée dans une mémoire réinscriptible ($E_2PROM$) d'un composant électronique, ledit composant électronique étant apte à effectuer des opérations susceptibles de modifier ladite donnée, caractérisé en ce que ledit procédé comporte les étapes suivantes :

a) dans une phase d'initialisation :

- définir dans ladite mémoire réinscriptible ($E_2PROM$) :
  - une zone (ZE) d'écriture de la donnée,
  - une zone (ZS) de sauvegarde de la donnée, dans laquelle est inscrite une valeur non corrompue de ladite donnée,
  - une zone (Zi) d'indication de restauration, dans laquelle est inscrite une valeur d'un indicateur (INR(Zi)) de restauration,
- définir dans une mémoire morte (ROM) du composant électronique une valeur (INR(1)), dite restauration, de l'indicateur (INR(Zi)) de restauration, indiquant qu'une restauration de la donnée doit être effectuée suite à une corruption d'écriture de ladite donnée,
- définir une valeur (INR(0)), dite d'effacement, de l'indicateur (INR(Zi)) de restauration, différente de la valeur (INR(1)) de restauration,

b) à chaque accès de ladite zone (ZE) d'écriture :

- lire dans la zone (Zi) d'indication de restauration la valeur dudit indicateur (INR(Zi))de restauration,
- si la valeur de l'indicateur de restauration est égale à ladite valeur (INR(1)) de restauration, effectuer une restauration de la donnée en inscrivant dans la zone (ZE) d'écriture la valeur de la donnée inscrite dans ladite zone (ZS) de sauvegarde et inscrire dans la zone (Zi) d'indication de restauration ladite valeur (INR(0)) d'effacement de l'indicateur de restauration.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre les étapes consistant, à chaque mise à jour de ladite zone (ZE) d'écriture, à :

- sauvegarder la valeur de ladite donnée inscrite dans la zone (ZE) d'écriture en l'inscrivant dans la zone (ZS) de sauvegarde,
- inscrire dans la zone (Zi) d'indication de restauration ladite valeur (INR(1)) de restauration,
- inscrire dans la zone (ZE) d'écriture une nouvelle valeur de la donnée, résultant de l'opération,
- inscrire dans la zone (Zi) d'indication de restauration ladite valeur (INR(0)) d'effacement de l'indicateur de restauration.

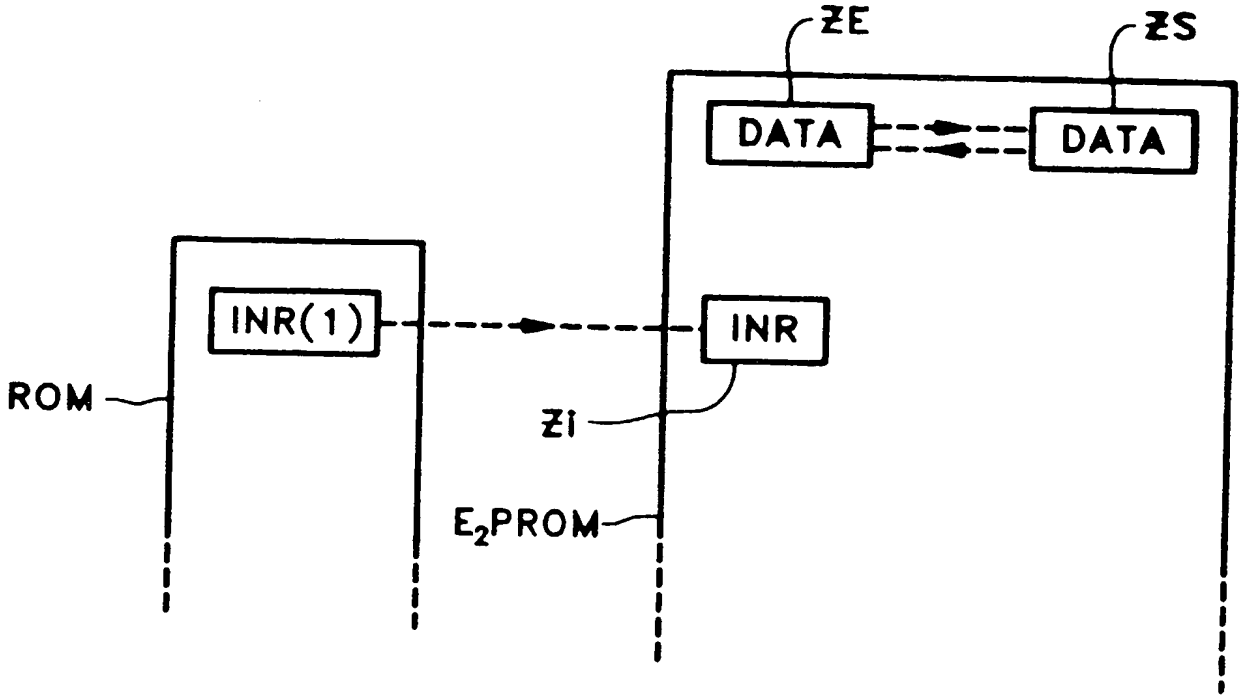



FIG.1

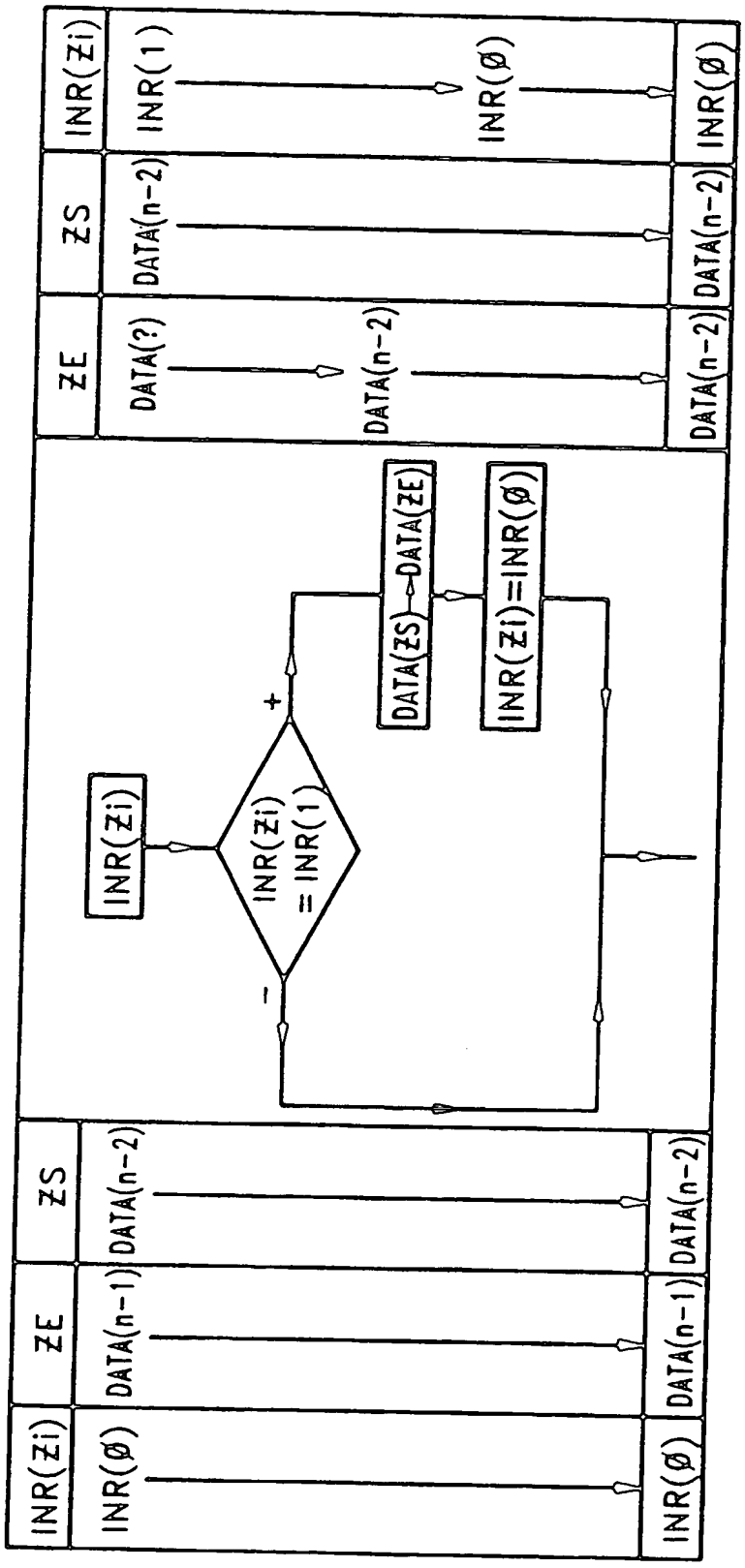



FIG.2

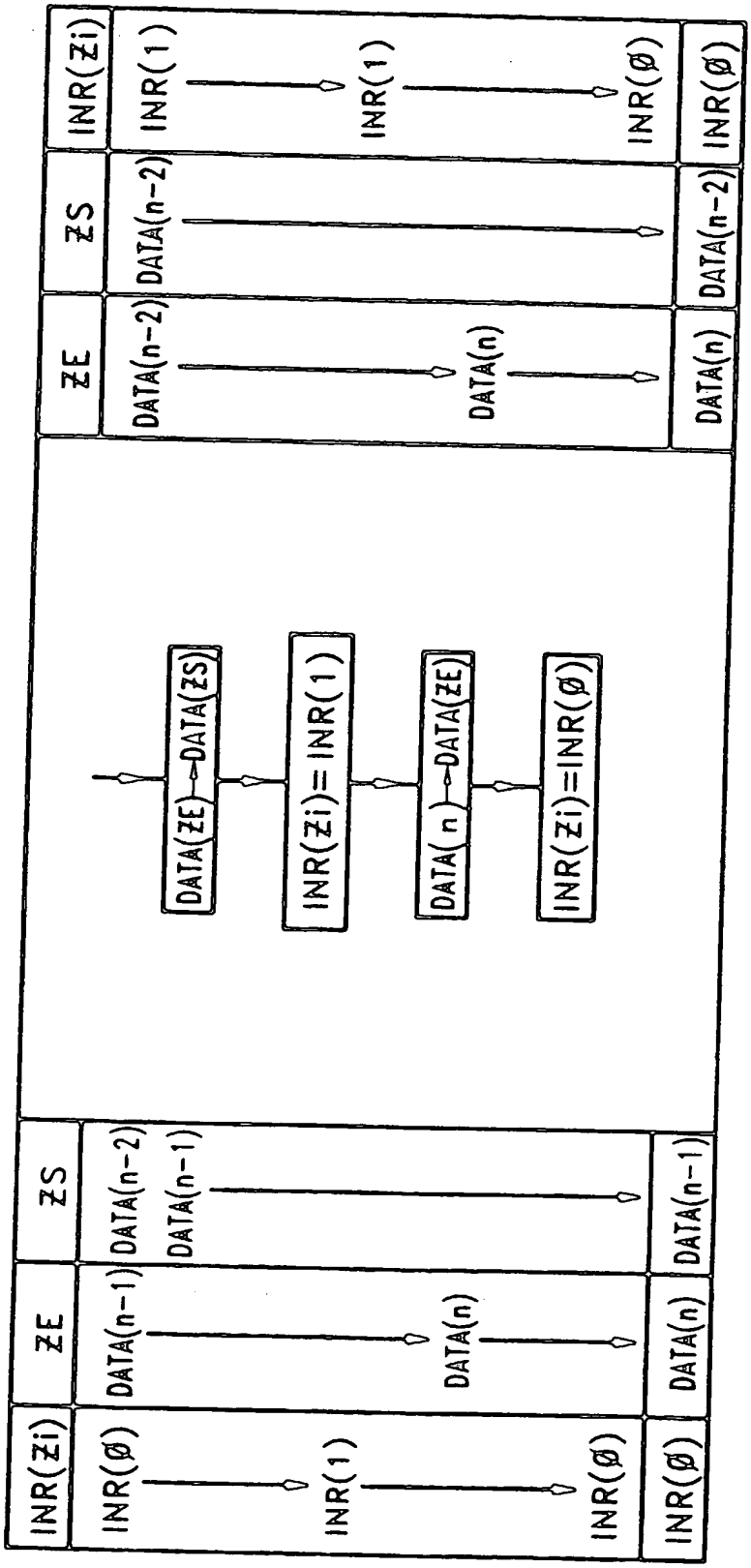



FIG.3

2757978

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

# RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 537295
FR 9616243

| DOCUMENTS CONSIDERES COMME PERTINENTS | | Revendications concernées de la demande examinée |
|---|---|---|
| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | |
| A | WO 96 25743 A (GEMPLUS CARD INT ;LAGET ANNE (FR); VALADE JEAN MARIE (FR)) 22 Août 1996<br>* abrégé *<br>* page 1, ligne 1 - ligne 15 *<br>* page 3, ligne 6 - page 5, ligne 12 *<br>* page 9, ligne 17 - page 10, ligne 22 *<br>* page 11, ligne 12 - page 14, ligne 4 *<br>* figure 2 *<br>--- | 1,2 |
| A | WO 94 24673 A (JONHIG LTD ;EVERETT DAVID B (GB); JACKSON KEITH M (GB); MILLER IAN) 27 Octobre 1994<br>* figure 1 *<br>* page 8, ligne 24 - page 10, ligne 13 *<br>* page 2, ligne 14 - ligne 22 *<br>* abrégé *<br>--- | 1,2 |
| A | EP 0 630 027 A (SOLAIC SOCIETE ANONYME) 21 Décembre 1994<br>* le document en entier *<br>----- | 1,2 |

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G07F
G11C
G06F

1

Date d'achèvement de la recherche: 5 Septembre 1997

Examinateur: Masche, C

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)